

PATENT ABSTRACTS OF JAPAN

(11)Publication number : 04-268937
(43)Date of publication of application : 24.09.1992

(51)Int.Cl. G06F 15/00
// G06F 15/62

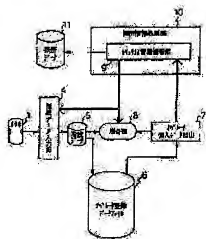
(21)Application number : 03-030047 (71)Applicant : TOSHIBA CORP
(22)Date of filing : 25.02.1991 (72)Inventor : HONDA YOJI

(54) SECRET INFORMATION PROCESSING SYSTEM

(57)Abstract:

PURPOSE: To provide a secret information processing system capable of accurately recognizing an operator and storing highly secret information.

CONSTITUTION: The secret information processing system is provided with a mouse 1 with a CCD sensor for reading out an operator's finger print, an operator data file 6 in which operator setting identification(ID) data added to the read finger print are previously registered and a secret information processing part 10 for collating the finger print data read out by the mouse 1 with finger print data stored in the file 6 by a collating part 8 at the time of accessing secret information previously set up in the system side, and when the operator is a certified person, allowing system start and access to secret data 11 and repeatedly checking the continuation of the same operator up to the end of the operation.



LEGAL STATUS

[Date of request for examination]
[Date of sending the examiner's decision of rejection]
[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]
[Date of final disposal for application]
[Patent number]
[Date of registration]
[Number of appeal against examiner's decision of rejection]
[Date of requesting appeal against examiner's decision of rejection]
[Date of extinction of right]

(19) 日本国特許庁 (J P)

(12) 公 開 特 許 公 報 (A)

(11) 特許出願公開番号

特開平4-268937

(43) 公開日 平成4年(1992)9月24日

(51) Int.Cl.⁵

G 0 6 F 15/00

/ G 0 6 F 15/62

識別記号

3 3 0 F 7323-5L

4 6 0 9071-5L

庁内整理番号

F I

技術表示箇所

審査請求 未請求 請求項の数2(全5頁)

(21) 出願番号 特願平3-30047

(22) 出願日 平成3年(1991)2月25日

(71) 出願人 000003078

株式会社東芝

神奈川県川崎市幸区堀川町72番地

(72) 発明者 本田 洋二

東京都府中市東芝町1番地 株式会社東芝

府中工場内

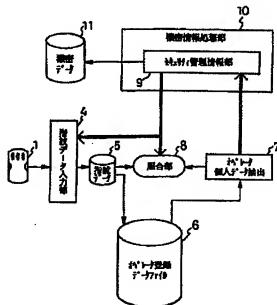
(74) 代理人 弁理士 三好 秀和 (外4名)

(54) 【発明の名称】 機密情報処理システム

(57) 【要約】

【目的】 オペレータ認識を適確に行い高度な機密保持を可能とする機密情報処理システムを提供することを目指す。

【構成】 オペレータの指紋を読み込むためのCCDセンサ付マウス1と、読み取られた指紋にオペレータ設定のための識別データを付加してあらかじめ登録したオペレータ・データファイル6と、あらかじめシステム側に設定された機密情報のアクセスの際には、CCDセンサ付マウス1で読み取られた指紋データとオペレータ・データファイル6内の指紋データとを照合部8で照合し、オペレータが認定された個人である場合にはシステム起動および機密データ11へのアクセスを許可するとともに、終了まで同一オペレータであることを反復確認する機密情報処理部10とを備えている。



【特許請求の範囲】

【請求項1】 オペレータの指紋を読み込むための指紋読取り手段と、読み取られた指紋にオペレータ設定のための識別データを付加してあらかじめ登録したオペレータ・データファイルと、あらかじめシステム側に設定された機密情報のアクセスの際には、指紋読取り手段で読み取られた指紋データとオペレータ・データファイル内の指紋データとを照合し、オペレータが認定された個人である場合にはシステム起動および機密データへのアクセスを許可するとともに、終了まで同一オペレータである

ことを特徴とする機密情報処理システム。
【請求項2】 上記指紋読取り手段は、指が把握する左、右側面部に丸みを持たせた切り込みをつけ、その部分に指紋読取り用のCCDセンサを取り付けたマウスであることを特徴とする請求項1記載の機密情報処理システム。

【発明の詳細な説明】

【0001】 【発明の目的】

【0002】

【産業上の利用分野】 本発明は、オフィスオートメーション機器等の機密保護を確実に行うことのできる機密情報処理システムに関する。

【0003】

【従来の技術】 たとえば、エンジニアリング・ワークステーション（以下EWSと略す）等の機器の多くは、内部データの機密保護または運用経費管理のため、使用するオペレータを限定する方法として、パスワードをキーボードから入力する方法や、暗号化する方法などが用いられている。

【0004】 パスワードを入力する方法を採用した際に問題となるのは、キーボードから入力されるパスワードが正しいか否かの判定により、オペレータが認定者か否かを識別する方法であるため、認定されたオペレータ以外でもパスワードを知りさえすれば、内部データへのアクセスが可能になってしまう。

【0005】 また、暗号化する方法は、複雑で手間がかかる、必ずしも100%解読されないという保証はない。

【0006】

【発明が解決しようとする課題】 このように、上記従来の方式では完全な機密保護を期待することはできないという問題点があった。

【0007】 本発明は、このような従来の問題点に鑑み、オペレータを指紋識別して正確に確認した上で、機密データへのアクセスを許可し、オペレータがアクセス中も、システム側から反復して認証作業を続けるようにして、高度な機密保持を実行することのできる機密情報処理システムを提供することを目的としている。

【0008】 【発明の構成】

【0009】

【課題を解決するための手段】 上記の目的を達成するため、本発明は、オペレータの指紋を読み込むための指紋読取り手段と、読み取られた指紋にオペレータ設定のための識別データを付加してあらかじめ登録したオペレータ・データファイルと、あらかじめシステム側に設定された機密情報のアクセスの際には、指紋読取り手段で読み取られた指紋データとオペレータ・データファイル内の指紋データとを照合し、オペレータが認定された個人である場合にはシステム起動および機密データへのアクセスを許可するとともに、終了まで同一オペレータであることを反復確認する機密情報処理手段とを備えたものである。

【0010】 また、上記指紋読取り手段は、指が把握する左、右側面部に丸みを持たせた切り込みをつけ、その部分に指紋読取り用のCCDセンサを取り付けたマウスであることを特徴とする。

【0011】

【作用】 上記の構成によれば、CCDセンサ付マウスにより指紋を読み取り、確実にオペレータの識別ができるようになり、内部オペレータ識別データと照合され、オペレータを判別することで、オペレータが限定され、またアクセス時間も短縮されて、確実な経費管理ができるようになる。

【0012】 オペレータがアクセス中も並行して、システム側からのオペレータ識別、確認手続きが反復されるので、高度な機密保護ができる。

【0013】

【実施例】 以下、本発明の一実施例を図面に基いて説明する。

【0014】 図1は、本発明に係る機密情報処理システムの一実施例の構成図である。また、図2は、本発明の一実施例が適用されるマウスの構成を示しており、図2(A)はマウスの上面図、図2(B)は図2(A)のa-a'の断面図であり、図2(C)はマウスの側面図である。

【0015】 初めに、マウス1の構成を説明すると、このマウス1はEWSの専用シート上で操作する光学式のマウスであり、このマウス1には実行を指示する際の選択ボタン2と、指紋検出用のCCDセンサ3が設けられている。

【0016】 マウス1の左右側面部には、指がフィットするような丸みを持たせた切り込みをつけ、その部分に指紋検出用CCDセンサ3が取り付けられている。

【0017】 したがって、オペレータはシステムを操作する際、通常、マウス1を選択ボタン2のセンターボタンが中指にくるように、上から利き手で押えて操作する。親指が置かれる丸みの切込み部分の位置には、CCDセンサ3が備わっているため、随時、親指の指紋を読み取ることが可能となる。

3

【0018】CCDセンサ3をマウス1の側面部の左右に設けたのは、左利き、右利きを想定して通常の操作上で、親指の指紋を検出できるようにするためである。

【0019】また図2(A)、(B)に示すように、親指がフィットするように、丸みを持たせておけるのは、CCDセンサ3を平面配置した場合と比較して、オペレーション時に指の挟まる面積を広くとって、指紋照合のための読み込みデータ量を増やすためである。

【0020】従来の指紋照合装置の水準では、通常人間の1指当りの指紋が有する特徴点(マニユージャ)は、約100個でありその中の約10個の相互照合合致点があれば、指紋が一部分しか検出できなくても、完全に個人を特定出切る精度にあるので、この場合は、充分に余裕のある検出レベルに設定してある。

【0021】なお、本実施例では、通常の操作を基準とし、利き手の親指の指紋を照合対象として説明したが、基本的に、いずれの指の指紋でも登録すれば、全く同様な効果を得ることはいふまでもない。

【0022】図1において、指紋データ入力部4は、上記マウス1で検出されたオペレータの指紋データを取り

込んで指紋データメモリ5へ送る機能を有する。
【0023】また、本実施例は、オペレータ認定登録手段としては、作成した指紋データを記憶しておき、キーボードから入力する個人識別データと組み合わせで保管する指紋データメモリ5と、指紋データ個人データをオペレータ登録として格納するオペレータ認定登録データファイル6とを備えている。

【0024】さらに、本実施例は、登録データファイル6からオペレータ個人データを抽出する個人データ抽出部7と、オペレータが入力した指紋データと、ファイル6から抽出した個人データとの照合を行う照合部8と、セキュリティ管理情報部9を含む機密情報処理部10と、この機密情報処理部10により管理される機密データファイル11とを備えている。

【0025】セキュリティ管理情報部9は、照合の結果、本人と確認されれば機密データファイル11へのアクセスを許可し、以後アクセスが終了してデータが出力されるまでの間、オペレータが入力して来る指紋データと、抽出してある個人データとの照合を反復繰返し行い、常に入力を監視、入力許可、アクセス排除、ロギング等、全てのセキュリティ管理を受け持つ。

【0026】このように構成された本実施例の作用について、つぎに説明する。

【0027】図3は、オペレータ認定登録の処理手順を示すフローチャートである。

【0028】初めに、キーボードやカードキーを使って、パスワードによるシステムの起動を行うとする(ステップS11)。

【0029】オペレータは、マウス1の選択操作によりディスプレイ上に、オペレータ登録実行を設定する(ス

4

テップS12)。

【0030】指紋データ入力部4は、マウス1のCCDセンサ3で検出した指紋を読み込み、指紋データを作成する(ステップS13)。次に、作成した指紋データをディスプレイ上に表示し、パスワード、ID番号等の個人識別データを付加する(ステップS14)。

【0031】このように作成して指紋、個人データは、指紋データメモリ5から、オペレータ登録ファイル6に転送し格納される。

【0032】また、上記のオペレータ登録の際に、個人データは必要に応じて、オペレータ個人々の資格別に、アクセス権の種類毎、アクセス可能なデータの範囲、参照権、更新権などの、細かに規制データも含めて、たとえば、グループ別、個人別に分けたアクセス資格の段階的付与処理を設定して、セキュリティ機能も高めることが可能である。

【0033】次に、図4に示す機密情報処理オペレーションのフローチャートに基づき、実際にオペレータが機密情報にアクセスする手順について説明する。

【0034】まず、システムを起動して、マウス1の選択で、処理実行用アイコンの「データ出力実行」を設定する(ステップS11、12)。

【0035】オペレータからの入力を受けて、機密情報処理部10のセキュリティ管理情報部9は、オペレータの確認指示の指令を出す(ステップS13)。

【0036】システムは、オペレータの識別処理として、個人データ抽出部7で抽出したファイル内指紋データと入力されたオペレータの指紋データとが、照合部8で照合され、許可判定が行われる。

【0037】ここで登録本人と判定されなければ(ステップS14拒否)、アクセスは不許可となり、セキュリティ管理情報部9の指令によって、システムは入力拒否をとり、システム起動画面に戻されて機密は保護される。本人と判定(ステップS14許可)の時は機密データファイル11へのアクセスが許可され、機密情報を読み出し、データとして出力される(ステップS15、16)。

【0038】また、機密情報処理部10はオペレータがアクセス中に、データを出力して作業が終了まで、オペレータに意識させることなく、オペレータのアクセスと並行して、ステップS13とステップS14のオペレータ確認作業を反復する。

【0039】若しも、アクセス中にオペレータの入力指紋データに変更が生じたら、直ちにセキュリティ管理情報部9の指令によって、アクセスを中止させ起動画面に戻すことで機密を保護する。

【0040】このように、システムとしてはオペレータが認定者である場合は、指紋照合によりオペレータが特定できるため、何時、誰が、どのシステムを操作したかを詳細に把握できるので、経費管理が従来に比べて大変

し易くなる。

【0041】この処理については、周知のロギングをセキュリティ管理部門が記録することで実行している。

【0042】なお、本実施例では、マウス1の両側面にCCDセンサ3を設けたが、マウス1の選択ボタン2や、キーボード上にCCDセンサ3を設けて、個人毎のアクセス権種別を組合わせて使用することも勿論可能である。

【0043】また、システム起動をパスワード等により、ログインの上で本発明のオペレータ認識を併用する10ように限定すれば、事前にオペレータを限定して、認定ファイルからデータ抽出できるから、オペレータ認識精度が向上し、高速処理が可能で効果的である。。

【0044】また、本発明の場合オペレータがマウス1を把持するだけで、オペレータ認識がされるために、自動ログインが可能となる。

【0045】

【発明の効果】以上説明したように本発明によれば、従来のセキュリティ方式がシステム起動初期時のみだったのと比較して、システム起動後機密データのアクセス時など、必要に応じてオペレータに意識されることなく、通常のマウス操作のまま、オペレータ識別を行うことができ、またオペレータ個々の資格に応じたアクセス権によって起動できるシステムを限定できるので、高次元の機密保護機能が得られ、アクセス時間の短縮へもつなが

る。

【0046】また、自動的にオペレータ認識が行えるために、システムのアクセス状態を詳細に把握することができ、経費管理を容易に行うことができる。

【図面の簡単な説明】

【図1】本発明の一実施例を示す構成図である。

【図2】本発明のCCDセンサ付マウスの構造説明図である。

【図3】本発明のオペレータ認定登録手順を示すフローチャートである。

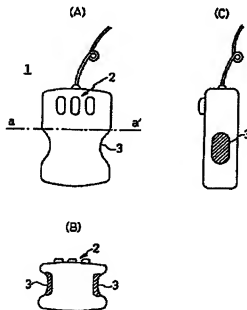
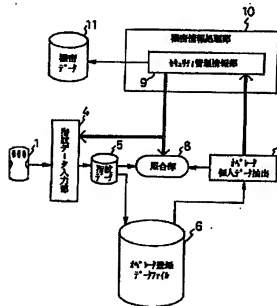
【図4】機密情報オペレーションの処理手順を示すフローチャートである。

【符号の説明】

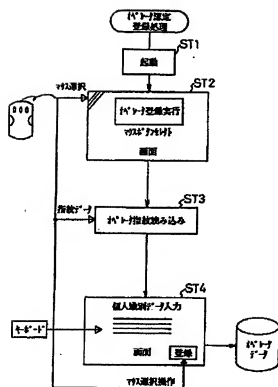
- 1 マウス本体
- 2 選択ボタン
- 3 指紋検出用CCDセンサ
- 4 指紋データ入力部
- 5 指紋データメモリ
- 6 オペレータ登録データファイル
- 7 オペレータ個人データ抽出部
- 8 照合部
- 9 セキュリティ管理情報部
- 10 機密情報処理部
- 11 機密データファイル

【図1】

【図2】



【図3】



【図4】

